

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号
特表2002-513245
(P2002-513245A)

(43) 公表日 平成14年5月8日(2002.5.8)

(51) Int. Cl.⁷ 識別記号

H 0 4 L 12/46
12/28
12/18

F I

H 0 4 L 11/00

11/18

データポート (参考)

3 1 0 C

審査請求 未請求 予備審査請求 有 (全 55 頁)

(21) 出願番号 特願2000-546493(P2000-546493)
(86) (22) 出願日 平成11年4月22日(1999.4.22)
(86) 優先文提出日 平成12年10月12日(2000.10.12)
(86) 国際出願番号 P C T / J S 9 9 / 0 8 8 6 6
(87) 国際公開番号 W O 9 9 / 5 6 4 3 6
(87) 国際公開日 平成11年11月4日(1999.11.4)
(31) 優先権主張番号 0 9 / 0 6 7 , 7 6 1
(32) 優先日 平成10年4月27日(1998.4.27)
(33) 優先権主張国 米国 (U S)

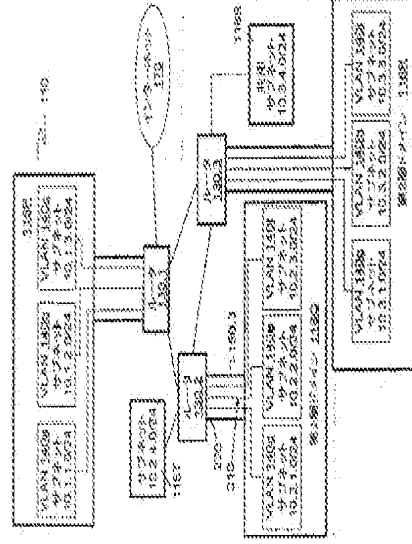
(71) 出願人 インターエヌエイビー・ネットワーク・サ
ービシズ・コーポレイション
I n t e r N A P N e t w o r k S e
r v i c e s C o r p o r a t i o n
アメリカ合衆国ワシントン州98101-
4064・シアトル・スイート 1000・デンス
フロア・ツェンニオンスクエア・ユニオン
ストリート 601
(72) 発明者 マクニール、トーマス・ジ
アメリカ合衆国ユタ州84097・オーレム・
イースト 1000ノース 1072
(74) 代理人 弁護士 大島 陽

(54) 【発明の名称】 ネットワークにおける接続の確立

(57) 【要約】

幾つかのドメイン (「第2層ドメイン」) を含む所定のネ
ットワークが、ルータによって相互接続される。各ドメ
インにおいて、トラフィックはMACアドレス (又は、他
のデータリンク層アドレス) に基づき送信される。ルー
タは、IPアドレス又は他のネットワーク層アドレスに基
づきトラフィックの経路を指定する。ネットワークの接
続を制限するために、ネットワーク管理者は、通信を許
可されたサブネットワークの集まりである各接続グル
ープを指定する。また、管理者は、どのエンティティ (M
A C アドレス、ポート、又はユーザ名) が同じグループに
属するかを指定する。そのエンティティは、同一のドメ
インか或いは異なるドメインに存在し得る。コンピュ
タシステムは、ルータに対してアクセス制御リストを自
動的に作成し、管理者の指定に従ってトラフィックを許
容又は拒否する。また、コンピュタシステムはVLANを
生成し、指定に従ってトラフィックを許可又は拒否す
る。ここで、各VLANはドメインの一部か或いはドメイ
ン全体である。各ドメインにおける接続性はVLANにより制
限され、またドメイン間の接続性はアクセス制御リス

最終頁に続く



【特許請求の範囲】

【請求項1】 ネットワーク端末をバーチャル同報通信ドメイン（VBDS）

に接続するための方法であって、

ネットワーク上においてネットワーク端末のユーザを識別する情報を前記ネットワーク端末から受信する過程と、

1以上のVBDを含むユーザの属する接続グループを決定する過程と、

前記ネットワーク端末が接続される1以上のVBDを決定する過程であって、前記1以上のVBDが前記接続グループのメンバーであるような前記決定過程と、

前記ネットワーク端末を前記1以上のVBDに接続するためのコマンドを発行する過程とを含むことを特徴とする方法。

【請求項2】 各VBDが、前記トラフィックが生じる前記VBDへの同報通信トラフィックを制限可能なドメインのサブドメインであり、

前記接続グループが、少なくとも2つのドメインからのVBDを含み、

前記ネットワーク端末が接続された1以上のVBDが、前記ネットワーク端末を含む前記ドメインに基づき決定されることを特徴とする請求項1に記載の方法。

【請求項3】 各VBDがVLANであり、また前記ネットワーク端末が、前記接続グループに属するVLAN並びに前記ネットワーク端末を含む前記ドメインに接続されることを特徴とする請求項2に記載の方法。

【請求項4】 ネットワーク端末をバーチャル同報通信ドメイン（VBDS）

に接続するための構造体であって、

ネットワーク上においてネットワーク端末のユーザを識別する情報を前記ネットワーク端末から受信する手段と、

1以上のVBDを含むユーザの属する接続グループを決定する手段と、

前記ネットワーク端末が接続される1以上のVBDを決定する手段であって、前記1以上のVBDが前記接続グループのメンバーであるような前記決定手段と、

前記ネットワーク端末を前記1以上のVBDに接続するためのコマンドを発行する手段とを含むことを特徴とする構造体。

【請求項5】 各VBDが、前記トラフィックが生じる前記VBDへの同報通信トラフィックを制限可能なドメインのサブドメインであり、

前記接続グループが、少なくとも2つのドメインからのVBDを含み、

前記ネットワーク端末が接続された1以上のVBDが、前記ネットワーク端末を含む前記ドメインに基づき決定されることを特徴とする請求項4に記載の構造体。

【請求項6】 各VBDがVLANであり、また前記ネットワーク端末が、前記接続グループに属するVLAN並びに前記ネットワーク端末を含む前記ドメインに接続されることを特徴とする請求項5に記載の構造体。

【請求項7】 前記構造体が、(1) 所定のコンピュータシステム、及び(2) 前記コンピュータシステムにロードされた所定のプログラムの含み、前記コンピュータシステム及び前記プログラムが、前記決定手段の各々を含むことを特徴とする請求項4に記載の構造体。

【請求項8】 前記構造体が、所定のコンピュータの読取り可能な媒体であり、そこで各手段が、1以上のコンピュータの命令、コンピュータの読取り可能なデータ、又は1以上の命令及びデータの組合せを含むことを特徴とする請求項4に記載の構造体。

【請求項9】 ネットワークドメイン間のトラフィックの経路を指定する1以上の装置に対して1以上のアクセス制御リスト (ACLs) を生成するための方法において、そのような装置にACLが与えられた場合に、前記装置が、前記ACLを用いて前記ドメイン間においてどのようなトラフィックが許可及び/又は拒否されるかを決定し、更に、

サブネットワークの各グループ内においてトラフィックが許可されるように、サブネットワークの1以上のグループを規定する過程であって、各サブネットワークがネットワークドメインの一部であるか、或いはネットワークドメインの全であり、また各グループに対して、所定のコンピュータシステムに前記グループに属するサブネットワークの識別子を与えるような前記過程と、

前記コンピュータシステムが、各グループ内のトラフィックを許可するため1以上のACLを生成する過程とを含むことを特徴とする方法。

【請求項10】 前記1以上のACLが異なるグループにおけるサブネットワーク間のトラフィックを拒否する前記複数のグループを規定する過程を含むことを特徴とする請求項9に記載の方法。

【請求項1 1】 1以上の共用サブネットワークの識別子を受信する前記コンピュータシステムを更に含む前記方法において、トラフィックが、前記グループの何れか1つにおける各共用サブネットワークと任意の別のサブネットワークの間において許可され、

1以上のACLによって、トラフィックが、前記グループの何れか1つにおける前記共用サブネットワークの何れか1つと任意のサブネットワークとの間において許可されることを特徴とする請求項9に記載の方法。

【請求項1 2】 少なくとも1つの前記ドメインが、前記ドメインにおけるトラフィックを制限することが可能であるような前記方法であって、

1以上のグループの各々に対して、前記コンピュータシステムが、前記グループ内において許可及び／又は拒否されたトラフィックを識別するための情報を受信する過程であって、前記情報が、制限するトラフィックにおける1以上のドメインによって使用されるような前記受信過程と、

前記情報による指定に従ってトラフィックを許可及び／又は拒否するように、前記コンピュータシステムがトラフィックを制限可能な各ドメインを構成する過程とを更に含むことを特徴とする請求項9に記載の方法。

【請求項1 3】 所定のグループ内において許可及び／又は拒否されたトラフィックを識別するための情報が、1以上の（1）トラフィックを制限可能なドメイン内のトラフィックを各々送信する1以上のスイチのポートであって、前記グループ内のトラフィックを運ぶための前記ポートと、（2）前記グループに属するエンティティの物理的アドレスと、更に（3）前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項1 2に記載の方法。

【請求項1 4】 各サブネットワークの識別子が、アドレス又はアドレスレンジであることを特徴とする請求項9に記載の方法。

【請求項1 5】 前記1以上の装置が、IPアドレスに基づきトラフィックの経路を指定し、また各ドメイン内において、トラフィックが物理的アドレスに基づき端末間で送信されることを特徴とする請求項9に記載の方法。

【請求項1 6】 ネットワークドメイン間のトラフィックの経路を指定す

る1以上の装置に対して1以上のアクセス制御リスト (ACLs) を生成するための所定の構造体において、そのような装置にACLが与えられた場合に、前記装置が、前記ACLを用いて前記ドメイン間においてどのようなトラフィックが許可及び／又は拒否されるかを決定し、更に、

各グループ内においてトラフィックが許可されるように、サブネットワークの1以上のグループをコンピュータシステムに対して規定する手段であって、各サブネットワークがネットワークドメインの一部であるか、或いはサブネットワークドメインの全でであり、また各グループに対して、前記グループに属するサブネットワークの識別子をコンピュータシステムによって読取るための前記規定手段と

前記コンピュータシステムによって、各グループ内のトラフィックを許可するために1以上のACLを生成するための手段とを含むことを特徴とする構造体。

【請求項17】 前記構造体が、前記コンピュータシステム及び該コンピュータシステムにロードされた所定のプログラムの含み、前記コンピュータシステムと前記プログラムとの組合せが、前記規定手段及び生成手段を含むことを特徴とする請求項16に記載の構造体。

【請求項18】 前記構造体が、前記規定手段及び前記生成手段を実施するための命令を含むコンピュータの読取り可能媒体であることを特徴とする請求項16に記載の構造体。

【請求項19】 前記規定手段が複数のグループを規定するときに、前記1以上のACLが異なるグループにおけるサブネットワーク間のトラフィックを拒否することを特徴とする請求項16に記載の構造体。

【請求項20】 1以上の共用サブネットワークの識別子を前記コンピュータシステムによって読取るための手段を更に含む前記構造体において、前記グループの何れか1つにおける各共用サブネットワークと他の任意のサブネットワークとの間でトラフィックが許可され、

1以上の前記ACLによって、前記グループの何れか1つにおける前記共用サブネットワークの何れか1つと任意のサブネットワークとの間でトラフィックが許可されることを特徴とする請求項16に記載の構造体。

【請求項21】 少なくとも1つの前記ドメインが、前記ドメインにおけるトラフィックを制限可能であるような前記構造体であって、

1以上のグループの各々に対して、前記グループ内における許可及び／又は拒否されたトラフィックを識別するための情報を前記コンピュータシステムによって読取るための手段であって、前記情報が、トラフィックの制限において1以上のドメインによって使用されるような読取り手段と、

前記情報に従ってトラフィックを許可及び／又は拒否するように、トラフィックを制限可能な各ドメインを前記コンピュータシステムによって構成するための手段とを更に含むことを特徴とする請求項16に記載の構造体。

【請求項22】 所定のグループ内において許可及び／又は拒否されたトラフィックを識別するための情報が、1以上の(1)トラフィックを制限可能なドメイン内のトラフィックを各々送信する1以上のスイッチのポートであって、前記グループ内のトラフィックを運ぶための前記1以上のポートと、(2)前記グループに属するエンティティの物理的アドレスと、更に(3)前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項21に記載の構造体。

【請求項23】 各サブネットワークの識別子が、アドレス又はアドレスレンジであることを特徴とする請求項16に記載の構造体。

【請求項24】 前記1以上の装置が、IPアドレスに基づきトラフィックの経路を指定し、また各ドメイン内において、トラフィックが物理的アドレスに基づき端末間で送信されることを特徴とする請求項16に記載の構造体。

【請求項25】 複数のドメインを含む所定のネットワークにおける接続を確立するための方法において、少なくとも1つのドメインが、前記ドメインにおいて規定されたサブドメインを有することができ、前記ドメインによって、単一のサブドメイン内のトラフィックが許可されるが、サブドメイン間のトラフィックが拒否され、更に、

各グループ内においてトラフィックが許可されるように1以上の接続グループを規定する過程であって、少なくとも1つの接続グループに対して、コンピュータシステムに前記接続グループに属するトラフィックを規定する情報を与えるよ

うな前記規定過程と、

少なくとも1つの接続グループに対して、前記コンピュータシステムに前記接続グループのメンバーであるサブドメインの識別子を与える過程と、

少なくとも1つの接続グループに対して、前記サブドメインによって前記接続グループにおけるトラフィックが許可されるように、前記コンピュータシステムが、前記接続グループにおけるサブドメインを有する各ドメインを構成する過程とを含むことを特徴とする方法。

【請求項26】 トラフィックを規定する前記情報が、少なくとも1つのグループに対して、1以上の（1）単一のドメイン内のトラフィックを各々送信する1以上のスイッチのポートであって、前記グループ内のトラフィックを選ぶための1以上の前記ポートと、（2）前記グループのメンバーである端末の物理的アドレスと、更に（3）前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項25に記載の方法。

【請求項27】 各々のドメインを構成する過程が、前記グループにおけるサブドメインを有する単一のドメイン内のトラフィックを送信するスイッチについて、（a）前記グループのメンバーである端末の物理的アドレス間のトラフィックを許可するための、また（b）異なるグループのメンバーである端末の物理的アドレス間のトラフィックを拒否するための前記スイッチを構成する過程を含むことを特徴とする請求項26に記載の方法。

【請求項28】 複数のドメインを含む所定のネットワークにおける接続を確立するための構造体において、少なくとも1つのドメインが、前記ドメインにおいて規定されたサブドメインを有することが可能であり、前記ドメインによって、単一のサブドメイン内のトラフィックが許可されるが、サブドメイン間のトラフィックが拒否され、更に、

1以上の接続グループのセットにおける各接続グループに属するトラフィックを規定する情報をコンピュータシステムによって受信するための手段であって、トラフィックが各グループ内で許可されるような前記受信手段と、

少なくとも1つの接続グループについて、前記接続グループのメンバーであるサブドメインの識別子を前記コンピュータシステムによって受信する手段と、

少なくとも1つの接続グループについて、前記サブドメインによって前記接続グループにおけるトラフィックが許可されるように、前記接続グループにおいてサブドメインを有する各ドメインを前記コンピュータシステムによって構成するための手段とを含むことを特徴とする所定の構造体。

【請求項29】 トラフィックを規定する前記情報が、少なくとも1つのグループに対して、1以上の(1) 単一のドメイン内のトラフィックを各々送信する1以上のスイッチのポートであって、前記グループ内のトラフィックを運ぶための1以上の前記ポートと、(2) 前記グループのメンバである端末の物理的地址と、更に(3) 前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項28に記載の構造体。

【請求項30】 前記構造体が、前記コンピュータシステム及び該コンピュータシステムにロードされた所定のプログラムを含み、前記コンピュータシステムと前記プログラムとの組合せが、前記全ての手段を含むことを特徴とする請求項28に記載の構造体。

【請求項31】 前記全ての手段を実施するための命令を含むコンピュータの読取り可能媒体であることを特徴とする請求項28に記載の構造体。

【請求項32】 各ドメイン内のトラフィックが、端末の物理的地址に基づき端末間で送信され、またドメイン間のトラフィックが、端末の論理アドレスに基づき経路指定されることを特徴とする請求項28に記載の構造体。

【発明の詳細な説明】

【0001】

発明の背景

本発明はネットワークに関連するもので、また詳細にはネットワークにおける接続性の確立に係るものである。

【0002】

セキュリティ上の理由やネットワークの通信量を低減する目的で、幾つかのネットワークでは接続を制限している。従って、ネットワークにおける幾つかの端末が互いに通信を許可される一方で、別の端末は通信を許可されない。接続は、通信を許可された端末間の物理的な通信リンクが確立されることによって可能となるか、或いは通信を許可されていない端末間の物理的な通信リンクが確立されないことによって禁止され得る。しかし、これは各セットの接続の制限のための物理的リンクを個別に構成することが必要であるので実際のではない。従って、コマンドを発行してネットワーク装置を割当てることによってネットワークの接続性を確立する或いは変更するための技術が発達してきた。

【0003】

これについて図1及び図2に示す（これらの図には先行技術にはない本発明の幾つかの態様が示してある）。ネットワーク110は、大規模な組織の相互接続に適する企業ネットワークである。ネットワーク110には、「第2層ドメイン(layer 2 domains)」116P、116Q、116R、116S、116Tが含まれる（用語「第2層」は、D. Biererらの"NetWare 4 for Professionals" (1993)、1-9頁（ここで言及することにより本明細書の一部とする）に記載のOSI参照モデルのを指す）。同一の第2層ドメイン116に属する端末124（例えば、ドメイン116Pにおける端末124.1、124.2）は、それらのMACアドレス（「第2層」アドレス）を用いて互いに通信可能である。MAC（媒体アクセス制御）アドレスは、端末のネットワークインターフェースカード（NIC）に書込まれた物理的アドレスであるか、又はNICスイッチの設定によって確立された物理的アドレスである。全てのドメイン116又はその幾つかには、1以上のネットワークスイッチ（NICスイッチと混同しない）が含まれ得る。各ドメイン116のスイッチ128は

、端末のMACアドレスを用いて端末124間でトラフィックを送信する。

【0004】

異なる第2層ドメインにおける端末（例えば、端末124.1、124.3）は、MACアドレスのみを使用して互いに通信することはできない。それらは、論理アドレスであるIPアドレスを用いて通信する。ルータ130.1、130.2、130.3は、端末のIPアドレス（必要に応じてIPアドレスとMACアドレスとの間で変換される）に基づきドメイン116間のトラフィックの経路を指定する。

【0005】

幾つかのドメイン116においては、バーチャルLAN（即ち、VLAN）を用いて接続性を制限することができる。例えば、ドメイン116Pには3つのVLAN 140a、140b、140cが含まれる（図2）。ドメイン116Pにおける端末124は、それらが同一のVLANに属している場合のみ、第2層において（即ち、それらの第2層アドレスを用いて）互いに通信可能である。従って、図1に示すVLAN 140aに属する端末124.1、124.2は通信可能である。

【0006】

VLANは、LANスイッチ128によって実現される。詳述すると、スイッチ128は、同一のVLAN内の端末間のみでパケットを送信する。（スイッチ128は、VLANへのトラフィックを制限可能なので、「VLAN-capable」と称される。例えば、ドメイン116S、116Tのような幾つかの第2層ドメインには、非VLAN-capableスイッチが含まれ得る。）

異なる第2層ドメイン間の接続は、ルータ130によって制限される。ルータ130は、IPアドレスに基づき接続の制限を規定するアクセス制御リスト（ACLs）を使用する（例えば、K. Siyan及びC. Bareの“Internet Firewalls and Network Security”（1995）、187-192頁を参照）。

【0007】

アクセス制御リストの作成及びFVLANの規定は、ネットワーク管理者を混乱させる面倒なプロセスであり得る。このプロセスは、動的ネットワーク環境においては度々繰返されねばならず、そこでは端末、ユーザ、及びネットワークサービスが或る場所から別の場所へ移動し、又は物理的な移動なしに或る組織から他の組

織へ移され、或いは付加もしくは除去される。

【0008】

従って、ネットワークにおける接続の設定を容易にすることが望ましい。

【0009】

発明の開示

本発明は、ネットワークの接続を確立及び制御するための新しい方法とシステムを提供するものである。幾つかの実施例においては、VLAN及びアクセス制御リストの容易な生成が可能となる。

【0010】

幾つかの実施例においては、アクセス制御リストが管理端末(management station)によって作成される。管理端末は接続グループの規定を受信する。各接続グループ(connectivity groups)はサブネットワークのグループである。トラフィックは各グループの中で許可される。幾つかの実施例において、各サブネットワークはIPサブネットとして識別される。管理端末は、接続グループを規定する情報からアクセス制御リストを作成する。

【0011】

幾つかの実施例において、管理端末は共用サブネットワークの識別子を受信し、また任意の接続グループにおける任意のサブネットワークと共用サブネットワークとの間のトラフィックを許可するACLを生成する。

【0012】

幾つかの実施例において、管理端末は、例えばVLANのようなサブドメインを、ドメインを適切に構成することによって生成する。ネットワーク管理者は、ドメインを構成するためにそのグループに属するトラフィックを規定する各接続グループ情報に入力する。そのような情報の例には、同一の接続グループに属するエンティティ(例えば、スイッチのポート、ネットワーク端末のMACアドレス、又はログイン時にユーザによって指定されるユーザ名)のリストが含まれる。異なる接続グループからのエンティティは通信を許可されない。接続グループは、異なる第2層ドメインからのエンティティを含み得る。エンティティは、どのエンティティがどのVLANに属するかを指定することなしに、接続グループに対して割

当てられ得る。管理端末は、同一のグループにおける何れのエンティティが所定の単一のドメインに属するかを決定し、そのようなエンティティを適切なVLANに配置する。

【0013】

幾つかの実施例において、接続グループにおけるトラフィックを規定する情報には、第2層パケットのビットの値が含まれる。

【0014】

本発明は、第2層ドメイン、スイッチ、又はルータに限られるものではない。

本発明の他の特徴及び優位性については後述する。本発明は添付した請求の範囲で規定されるものである。

【0015】

発明の詳細な説明

ネットワーク110には、5つの第2層ドメイン116が含まれる。各ドメインにおけるパケットのアドレス指定が、OSI参照モデルの第2層（データリンク層）におけるパケットの内容に基づき行われるので、これらのドメインは「第2層」と称される。ルータ130は、第3層（ネットワーク層）におけるパケットの内容に基づきトラフィックの経路を指定する。特に、IPアドレスは、第3層のアドレスである。しかし、本発明は第2層若しくは第3層又はOSI参照モデルに従うネットワークに限定されるものではない。

【0016】

ドメイン116Pには、MACアドレスに基づきトラフィックを送信するVLAN-capableスイッチ128.1、128.2が含まれる。これらのスイッチは、トランク150.1によって互いに接続されている。各スイッチは、ネットワークセグメントに各々接続されている1以上のポートを有する。従って、スイッチ128.1のポート160.1は、端末124.1を含むネットワークに接続されている。また、スイッチ128.2のポート160.2は、端末124.2を含むネットワークに接続されている。図1において、各ネットワークセグメントは単一の端末を含む。或る実施例においては、ネットワークセグメントは複数の端末を含む。

【0017】

スイッチ128.1のポート1160Mは、後述するような接続グループの生成に用いられる管理端末124Mに接続される。

【0018】

スイッチ128.1は、トランク150.2によってルータ130.1に接続される。ルータ130.1は、ルータ130.2、130.3、及びインタンネットワーク170に接続される。ルータ130.2は、ルータ130.3に接続される。ルータ130.2は、トランク150.3によってドメイン116QのVLAN-capableスイッチ128.3に接続される。ドメイン116Qには、VLAN-capableスイッチ128.4、128.5、及び128.6が含まれ、その各々はスイッチ128.1、128.2と同様に1以上のネットワークに接続される。ここでは、端末124.3を含むセグメントのみを示す。また、ドメイン116Qのスイッチ128は互いに接続されている。

【0019】

ルータ130.2は、第2層ドメイン116Tに接続されている。

【0020】

ルータ130.3は、ドメイン116RのVLAN-capableスイッチ128.7及び第2層ドメイン116Sに接続されている。スイッチ128.7は、スイッチ128.1、128.2と同様にネットワークセグメント（図示せず）に接続されている。ドメイン116S、116Tはスイッチを全く含まないか、或いは幾つかのスイッチ（図示せず）を含む。

【0021】

幾つかの実施例において、1以上のドメイン116はスイッチを全く含まないか、或いは非VLAN-capableスイッチ、ハブ又はコンセントレータを含む。

【0022】

前述のように、異なるドメイン間の通信にはIPアドレスが使用される。例えば、端末124.3にパケットを送信するために、端末124.1は、端末124.3のIPアドレス及びルータ130.1のMACアドレスを、それぞれ論理的宛先アドレス及び物理的宛先アドレスとしてパケットに書込む。ルータ130.1は、宛先MACアドレスをルータ130.2のMACアドレスと置き換え、端末124.1の発信元MACアドレスをルータ130.1のMACアドレスに置き換える。次にルータ130.1が、パケットをルータ130.2に送

信ずる。ルータ130.2は、パケットの発信元MACアドレスを自身のMACアドレスに置き換え、また宛先MACアドレスを端末124.3のMACアドレスに置き換えて、パケットをスイッチ128.3に送信する。スイッチ128.3は、パケットをスイッチ128.5経由で端末124.3に送信する。ドメイン116Pには重複していないVLAN140a、140b、140c（図2）が含まれ、ドメイン116Qには、重複していないVLAN140d、140e、140fが含まれ、ドメイン116Rには重複していないVLAN140g、140h、140iが含まれる。VLANにおける端末のメンバシップは、端末が接続されているスイッチポート160によって規定されるか、端末のMACアドレスによって規定されるか、或いは端末にロギオンしたユーザのユーザ名によって規定される。ポート又はMACアドレスに基づくVLANのメンバシップの確定については、G. Heldの“Virtual LANs: Construction, Implementation, and Management”（1997）、233-249頁（ここで言及することにより本明細書の一部とする）に開示されている。

【0023】

ユーザ名によるVLANのメンバシップの確定については、付録Aに記載されている（“User-Based Binding of Network Stations to Broadcast Domains”と題するJ. Ekstromらの米国特許出願08/832,011（1997年4月2日出願；ここで言及することにより本明細書の一部とする）を参照）。或る実施例においては、VLAN140が、ポートによって識別される端末、MACアドレスによって識別される端末、及び／又はユーザ名によって識別される端末を結び付ける。

【0024】

ドメイン116S、116Tは、任意のVLANを含む場合もあり、また含まない場合もある。

【0025】

管理端末124Mは、VLAN140bに属する。端末124Mは、任意のスイッチ128及び任意のルータ130と通信可能である。或る実施例において、（1）全てのスイッチ128は、Cisco社（San Jose, California）から入手可能なtype CatalystTMのスイッチであり、また（2）ルータ130は、Cisco社から入手可能なルータであり、それらはCisco社の説明書に記載されている（部品番号7

8-2040-01)。これらは、ここで言及することにより本明細書の一部とする。

【0026】

ネットワーク110には、種々のドメイン116におけるエンティティ（非トランクスイッチポート160、MACアドレス、又はユーザ名）を含む接続グループが含まれる。例えば、接続グループは、VLAN140a、140d、140gにおける全てのエンティティによって構成され得る。通信は、同一の接続グループにおける全てのエンティティ間においては許可され、異なる接続グループにおけるエンティティ間においては拒否される。詳述すると、スイッチ128及びルータ130は、或る接続グループにおける端末124から別の接続グループにおける端末124へのパケットの経路は指定しない。

【0027】

周知のように、VLANは同報通信ドメインである（また、ここでは「第2層同報通信ドメイン」又は「第2層BD」と称される）。対照的に、接続グループは必ずしも同報通信ドメインではない。従って、幾つかの実施例においては、同報通信又はマルチキャストトラフィックは単一のVLANに制限される。

【0028】

また、本明細書においてVLANは「バッチャル同報通信ドメイン」即ちVBDと称される。VBDは、ネットワークにおいて必ずしも物理的な接続（例えば、ケーブル）の変更の必要なしに規定され得る同報通信ドメインである。

【0029】

管理端末124Mには、プログラムやデータを記憶するための記憶装置192、並びにキーボード、スクリーン、及び/又は他のインタフェース機器のようなユーザインタフェース機器194が含まれる。

【0030】

付録Bは、幾つかの実施例における接続グループを生成する（特に、VLAN140及びルータアクセス制御リストを生成する）プロセスを示している。ここで、このプロセスは図1のVLANの例に示しており、また3つの接続グループは以下の通りである。

【0031】

グループ1は、VLAN140a、140d、及び140gからなる。

【0032】

グループ2は、VLAN140b、140e、及び140hからなる。

(このグループは、管理端末124Mを含む管理接続グループとして指定され得る。)

グループ3は、VLAN140c、140f、及び140iからなる。

【0033】

幾つかの実施例においては、第2層ドメイン116Sは同報通信ドメインである。付録Bのプロセスは、ドメイン116Sを、任意の接続グループとの通信を許可された共用IPサブネットとして構成する。重要なことは、各第2層同報通信ドメインが、IPサブネット又はIPサブネットの組合せであることである。

【0034】

付録Bのプロセスは、第2層ドメイン116T及び関連するサブネットを「非管理(unmanaged)」状態にする(即ち、対応するルーティングテーブルに対してACLが生成されず、更にプロセスによって生成された任意のACLにおいてサブネット116Tは明示されない。)。従って、ドメイン116Tは任意の接続グループからトラフィックを受取り可能であるが、ドメイン116Tから任意の接続グループへのトラフィックは、ルーティング130によって取除かれ得る(遮断され得る)。

【0035】

幾つかの実施例において、単一の第2層ドメインには、管理されたサブネット及び非管理のサブネットが含まれる。

【0036】

付録Bのプロセスは、任意のVLAN又は接続グループがネットワーク110において確立される前か或いは確立された後に実施され得る。幾つかの実施例において、付録Bのプロセスが最初に実施され、全てのドメイン116(場合によって、ドメイン116S、116Tのような共用ドメイン及び非管理のドメインのエンティティを除く)における全ての通信エンティティを含む単一の「管理接続グループ(management connectivity group)」を確立する。その管理グループによっ

て、管理端末124Mが全てのスイッチ及びルータと通信可能となる。次に付録Bのプロセス又は付録Gのメンテナンspbプロセスが実施され、前述のグループ1、2、3又は別の任意のグループを確立する。そのようなグループの設置は、管理端末がスイッチ及びルータと通信する能力によって容易となる。

【0037】

或いは、管理端末124M及びスイッチ128のポートのみが管理接続グループに配置される。幾つかの実施例においては、スイッチ128のそれらのポートのみが管理接続グループに配置され、その管理接続グループは管理端末124Mを全てのVLAN-capableスイッチ及び全てのルータと通信可能とすることを要求される。

【0038】

後述する実施例においては、付録Bのプロセスの開始時に接続グループが存在しないと仮定する。

【0039】

付録Bのプロセスが開始される前に、各ルータ130が構成されて、1以上のIPサブネットが各ルータインタフェース210に割当てられる(図2)。(Cisco社の説明書において「サブインタフェース」と称される幾つかに対して、ここでは用語「インタフェース」を用いることに注意されたい。)付録Bのプロセスが完了した後に、各ルータ130は、それらが接続されるドメイン116の各VLAN140に対して個別のインタフェースを有し得る。

【0040】

各VLAN140はサブネット又はサブネットの組合せであるので、経路指定ソフトウェアがVLANを明確に認識しない場合でも、ルータ130がVLANに基づき事実上の送信決定を行うことに注意されたい。ルータは、ルータのトランクポート(例えば、トランクポート220)経由でドメインに接続され、また各インタフェースはトランクポートの論理的サブポートである。

【0041】

周知の通り、ルータ及びスイッチのトランクポート(即ち、スイッチ、又はスイッチ及びルータと相互接続するトランク150に接続されたポート)は、マル

サブVLANのためのトラフィックを運ぶ。トランクポートにおけるトラフィックはトランクプロトコル(trunking protocol)を使用し、そこで各パケットは、パケットが割当てられるVLANの識別子を認識したより大きなパケットにカプセル化(encapsulated)される。VLANメンバーシップがMACアドレスよりも寧ろポートによって規定される場合、VLANの認識によって受信スイッチ128がパケットのVLANを識別することが可能となる。

【0042】

ルータ130はトランクプロトコルを理解し、同一のトランクポートにおける種々のVLANからのトラフィックを、各VLANからのトラフィックがVLANに割当てられた個別のポートに到達した場合のように取り扱う。

【0043】

幾つかの実施例においては、トランクの代わりにルータと第2層ドメインとの間の個別の物理的接続を用いて個々のVLANに対するトラフィックを運ぶ。

【0044】

各インタフェースは、インタフェースによって取扱われる各サブネットにおけるゲートウェイアドレスを有する。ゲートウェイアドレスは、サブネットにおけるルータのアドレスである。

【0045】

付録Cは、記憶装置192において付録Bの幾つかのステップによって作成されたデータベースを示す。

【0046】

ステップM5 (付録B) において、ネットワーク管理者は、管理端末124Mにネットワーク110のIPアドレスレンジを与える。付録Bの例において、アドレスレンジは10.0.0.0/8である。ネットワーク110において、各サブネットは255.255.255.0のサブネットマスクを有する。

【0047】

IPアドレスレンジ及びサブネットは、形式10.0.0.0/8 (サブネットマスクは、全て0が続く有意な8つの1を有する) を有するか、或いはIPアドレス (10.0.0.0) 及びサブネットマスク (255.0.0.0) の組合せのような形式を有する。

【0048】

付録Cの11に示すように、管理端末124Mはネットワーク110のIPアドレスレンジをそのデータベースに入力する。

【0049】

付録Bに示すように、ステップM7が管理者によって実施される。端末124Mがデータベース12を生成する（付録C）。この情報及び付録Cにおける他の情報は、異なる実施例においては異なって編成される。例えば、幾つかの実施例において、項目12-1（スイッチのアドレス）は、各ドメインに対するアドレスのリストとして格納される。別の実施例においては、同様の情報は、アドレス及び各ドメインのペアとして格納される。別の実施例においては他のデータ構造が用いられる。

【0050】

ステップM10において、ネットワーク管理者がVLAN140を規定する。VLANの規定には、各ドメイン116における各スイッチ128及び端末124Mに対してVLAN識別子を与える過程が含まれる。VLAN識別子は、スイッチ128に認識可能な識別子（即ち、VLAN番号）である。例えば、スイッチ128.1、128.2の各々は、VLAN140a、140b、140cの識別子を受信し、スイッチ128.7は、VLAN140g、140h、140iの識別子を受信する。VLANを規定する過程には、何れのエンティティ（ポート、MACアドレス又はユーザ名）が各々のVLANに属するかを明らかにする過程は含まれない。

【0051】

或る実施例においては、管理者がVLAN識別子を各スイッチ128に直接入力する。別の実施例においては、管理者がVLAN識別子を各ドメイン116の制御スイッチ128に入力する。制御スイッチは、同一のドメインにおける別のスイッチ（仮に存在すれば）に対して識別子を送信する。更に別の実施例においては、管理者はこの情報を例えばTelnet又はSNMPプロトコルを用いて端末124Mから遠隔のスイッチ128に情報を与える。

【0052】

付録Cの13に示すように、端末124Mはこの情報をそのデータベースに格

納する。

【0053】

ステップM14において、ネットワーク管理者は情報14（付録C）を端末124Mに入力する。図1及び図2において、個々のサブネットは各第2層BDに割当てられ、第2層BDとIPサブネットとの間に1対1対応が存在する。サブネットは、図2及び次の表1に示されている。

【0054】

【表1】

表1

第2層BD	サブネット
140a	10.1.1.0/24
140b	10.1.2.0/24
140c	10.1.3.0/24
140d	10.2.1.0/24
140e	10.2.2.0/24
140f	10.2.3.0/24
140g	10.3.1.0/24
140h	10.3.2.0/24
140i	10.3.3.0/24
116S	10.3.4.0/24
116T	10.2.4.0/24

【0055】

幾つかの実施例においては、複数のサブネットが第2層BDに対して割当てられている。

【0056】

サブネットは、サブネットマスクの表記法、又はサブネットアドレス及びマスクの表記法における1のサブネットアドレス/番号を用いて端末124Mに与えられる。

【0057】

またステップM14において、対応するIPサブネットからの各VLANにおけるIPアドレスを割当てるためにネットワーク110が構築される。従って、幾つかのWindows NTTMの実施例において、DHCPサーバは各サブネットにおいてIPアドレスを割当てるために構成される。(Windows NTについては、例えばR. Sant' Angeloらの“Windows 3 NT Server Survival Guide” (1996)に記載されており、これについては、ここで言及することにより本明細書の一部とする。) 幾つかの実施例においては、DHCPサーバがルータ130においてサブネットの1つに接続される。ルータは、DHCPのリクエストをルータに直接接続された全てのサブネットからこのDHCPサーバへ送信するように構成される。別の実施例においては、個別のDHCPサーバが各サブネットに設けられる。

【0058】

ステップM20において、各接続グループに対して、管理者は接続グループのメンバであるIPサブネット (即ち、接続グループのメンバである第2層 BDの一部であるIPサブネット) を端末124Mに入力する。従って、管理者は、接続グループ1に対してVLAN140a、140d、140gにおけるサブネットを入力し、グループ2に対してVLAN140b、140e、140hにおけるサブネットを入力し、更にグループ3に対してVLAN140c、140f、140iにおけるサブネットを入力する。或いは、各接続グループに対して、管理者は、接続グループの第2層 BDメンバの識別子を入力する。各々のケースにおいて、全てのルータを管理端末124Mから到達可能とするために、管理者は、管理接続グループのメンバであるIPサブネットを入力し得る。幾つかの実施例において、各ルータは、共有サブネット又は管理接続グループのサブネットメンバにおける少なくとも1つのゲートウェイIPアドレスを有する。

【0059】

幾つかの実施例では、全てのルータが管理端末から到達可能であることを必要としない。従って、管理されていないサブネット及び他のルータにのみ直接接続されたルータは、幾つかの実施例においては到達可能であることを必要としない。

【0060】

項目15（付録C）が、ステップM20において生成される。

【0061】

多数のサブネットが単一の第2層BDに割当てられた場合、それらは全て同じ接続グループに割当てられる。

【0062】

ステップM30において、管理者が各接続グループに属するエンティティを端末124Mに入力する。ここで、I6（付録C）が生成される。例えば、接続グループ1の場合、管理者はスイッチポート160.1、160.2、160.3（ポート160.3に接続された端末124.3はVLAN140dに属すると仮定する）、及び他のポート、MACアドレス、並びに／又はVLAN140a、140d、140gに属するユーザ名を入力する。幾つかの実施例においては、管理者は、ポート、MACアドレス又はユーザ名がどのドメイン又はVLANに属するかを記憶する必要がない。

【0063】

ポート160は、参照が容易なように管理者によって割付けられ得るラベルによって、端末124Mにおいて識別される。例えば、ポートがユーザ名Fredのユーザによって使用される端末124に接続されている場合、管理者はそのポートにラベル「Fred」を割付けることができ、またステップM30において「Fred」を入力してこのポートを接続グループに割付けることが可能である。MACアドレスの接続グループへの割付も同様である。

【0064】

ステップM40において、管理者は情報17及び18（付録C）を管理端末124Mに入力する。

【0065】

ステップM45において、端末124MがVLAN140を生成し、付録Dに示すように各エンティティを適当なVLANに配置する。付録Dにおいて、括弧内の番号は、付録Dの対応するステップにおいて用いられる付録Cのデータベース項目を指す。

【0066】

付録Dにおいて、接続グループのエンティティEがVLAN-capableスイッチ（ステップV1）のポート160である場合、そのエンティティはポートが属するドメイン116のVLANにのみ配置される。対照的に、エンティティがMACアドレス（ステップV2）又はユーザ名（ステップV3）である場合、そのエンティティは接続グループの全てのVLANに配置される。MACアドレスの場合では、これによってMACアドレスを有する端末が、その接続グループのVLANを含む任意のドメイン116に接続され得る。従って、接続グループ1におけるMACアドレスを有する携帯用コンピュータ（例えば、ラップトップコンピュータ）は、ドメイン116P、116Q、116Rに接続され得る。コンピュータがドメイン116Pに接続される場合、発信元アドレスとしてコンピュータのMACアドレスを有するパケットを受信するスイッチ128.1、128.2によって、コンピュータがVLAN140aに配置され得る。同様に、例えばコンピュータがドメイン116Qに接続される場合、それはVLAN140dに配置され得る。

【0067】

同様に、ユーザ名が接続グループの全てのVLAN140に配置される。ユーザがドメイン116Pにログオンした場合、ユーザを適切なVLANに切替えるためにUBNCサーバに対する要求がドメイン116Pから届く。例えばユーザ名が接続グループ1に存在する場合、UBNCサーバはユーザをVLAN140aに配置する。同様に、ユーザがドメイン116Q又は116Rにログオンする場合、UBNCサーバは、ユーザをVLAN140d又は140gにそれぞれ配置する。

【0068】

ステップV3において、「実施例1」は接続グループに関連する任意の事項を知るためにUBNCサーバを必要としない。端末124Mは、各ドメイン116におけるユーザ名に対してどのVLANが割当てられるかをUBNCサーバに知らせる（ステップV3-2）。実施例2においては、UBNCサーバはどのVLANがどの接続グループに属するかを認識している（この情報はUBNCサーバに直接与えられるか、或いは例えば端末124Mから遠隔的に与えられ得る）。従って、実施例2のステップV3-1において、端末124MはどのVLANがユーザに割当てられるかをUBNCサーバに通知しない。ユーザがログオンした時、UBNCサーバはログオンが生じた

ドメイン116及びユーザの接続グループからユーザのVLANを決定する。UBNCデータベースには、各ドメイン116における各VLANに関連するIPサブネットが含まれるので、ドメイン116はユーザのIPアドレスから決定される。幾つかの実施例においては、UBNCサーバは管理端末124Mにおいて作動する。

【0069】

ステップM50（付録B）において、端末124Mは、付録Eにおけるプログラムを実行することによって、ルータアクセス制御リストを作成する。個別のアクセス制御リストが、接続グループのサブネット番号が直接結び付けられる各ルータインタフェースに対して作成される。付録Eのプログラムは、ルータ130、2からVLAN140eまでのインタフェース210の例において説明され得る。

【0070】

各ルータインタフェースに対して、対応するサブネットが所定の接続グループに属する場合、付録Fに示すようにステップA1からA5によってアクセス制御リストが作成される。付録Fにおける回線番号（例えば、AL1-1）は、付録Eのステップ番号に対応する。従って、例えばステップA1（付録E）は回線AL1-1を生成し、ステップA2は回線AL1-2a及びAL1-2bを生成する。

【0071】

付録Fは、Cisco社（San Jose, California）の幾つかのルータによって用いられるシンタクスを用いる。このシンタクスについては、K. Sliyan及びC. Hareの“Internet Firewalls and Network Security”（1995）、186-191頁に記載されており、これについてはここで言及することにより本明細書の一部とする。回線番号（例えばAL1-1）は、アクセス制御リストの一部ではない。更に、感嘆符「!」で始まり行の終わりをまたいで続く文章は、ルータによって無視されるコメントである。これらのコメントは幾つかの実施例においては省略される。

【0072】

ステップA1は、サブネット116Sのような各共用サブネットからのインタフェース210へのトラフィックを許可する回線を生成する。そのプログラムは、アクセス制御リストに対して、「アクセスリスト(access-list)」、アクセス

制御リスト番号（幾つかの実施例においてプログラム自身によって連続的に発生する）、「許可 ip (permit ip)」、共用サブネットのIPアドレス、並びに0.0.0.255のワイルドカードマスクを書き込む。（入力のパケットIPと比較して、ワイルドカードマスクにおける0ビットは、発信元IPアドレスの対応するビットが1ビットによって使用されていることを示し、ワイルドカードマスクにおける1ビットは、対応するビットが使用されていないことを示す。）

回線A L 1 - 1におけるワイルドカードマスク0.0.0.255は、サブネットマスクを反転させることによって決定される。

【0073】

ステップA 2は、同一の接続グループにおける他の全てのサブネット（即ち、第2層 BD）からのトラフィックを許容する例えば回線A L 1 - 2 a、A L 1 - 2 bのような回線を生成する。回線A L 1 - 2 aは、サブネット10.1.2.0/24（VLAN 1 4 0 b）からのトラフィックを許容する。回線A L 1 - 2 bは、サブネット10.3.2.0/24（VLAN 1 4 0 b）からのトラフィックを許容する。

【0074】

ステップA 3は、ネットワーク110における他の全ての端末からのトラフィックを拒否する回線A L 1 - 3を生成する。（重要なことは、ルータがパケットを受取ったときに、ルータがアクセス制御リストの始めからパケットの開始をテストすることである。パケットに適合する行が発見されたととき、アクセス制御リストの残りの部分は無視される。）ワイルドカードマスクは、ネットワーク110のIPアドレスレンジマスクを反転させることによって得られる。

【0075】

ステップA 4によって、インターネット170からのトラフィックを含むネットワーク110の外部の任意の端末からのトラフィックを許容する回線A L 1 - 4が生成される。

【0076】

幾つかの実施例において、管理者は、ステップM 5 0の前に接続グループにおける各サブネットに対して、インターネットからサブネットへのトラフィックが許可されるかどうかを管理端末124 Mに示す。トラフィックが拒否された場合

は、対応するインタフェースに対してステップA4が省略され、またステップA3がラインAL1-3の代わりの「任意の拒否ip (deny ip any)」国線を生成する。

【0077】

付録Eに示すようにステップA5が実施される。

【0078】

ルータインタフェースが接続グループのBDメンバに接続されずに、共用若しくは非管理サブネット（例えば160S）又はインターネット170に接続される場合、ACLは生成されずにサブネット若しくはインターネットは他の任意のサブネットからアクセス可能となる。

【0079】

幾つかの実施例においては、付録BのステップM40において、管理者は各共用サブネットに対してどのようなアクセスが与えられるかを指定し、付録Eのプロセスによって、当業者に周知の方法を用いて適切なアクセス制御リストが作成される。例えば、共用サブネットがネットワーク110の中からのみアクセス可能とされる場合、アクセス制御リストは以下のように構成され得る。

【0080】

アクセスリスト1許可ip 10.0.0.0 0.255.255.255

アクセスリスト1拒否ip 任意

別の実施例において、そのような機能性は、ルータ130.1又は他の幾つかの機器（図示せず）において具現される企業全体に広がるファイアウォールによって与えられる。

【0081】

管理端末124Mは、存在する全てのアクセス制御リストを消去して、新しいアクセス制御リストに置き換えるように各ルータ130に指示する。

【0082】

幾つかの実施例においては、ネットワーク管理者は追加のコマンドをアクセス制御リストに挿入することが可能である。従って、幾つかの実施例においては、管理者が、ステップM50の前に対応するインタフェースに対してアクセス制御

リストに挿入される各サブネットの追加項を指定し得る。詳述すると、管理者は、ステップA 1の前に挿入される項、ステップA 2とA 3の間で挿入される項、ステップA 3とA 4の間で挿入される項、及びステップA 4の後に挿入される項を指定することができる。幾つかの実施例において、この技術を用いてファイアウォールの機能をアクセス制御リストに組み込み、従って、企業全体に渡る個別のファイアウォールの必要はなくなる。

【0083】

幾つかの実施例においては、ステップM 10及びM 20が省略される。ステップM 45において、各接続グループに対して、管理端末124Mは、VLAN-capableスイッチ及び接続グループにおける1以上のエンティティを有する各ドメイン116においてVLANを生成し、またVLANにエンティティを配置する。(従って、ドメインが接続グループにおけるポート160を有する場合、或いは接続グループにMACアドレス又はユーザ名が含まれる場合に、VLANがドメインの中に生成される。) また端末124Mによって、IPサブネット(例えば、10.1.1.0/24)が、VLANに割当てられる。

【0084】

幾つかの実施例においては、VLANのメンバーシップは、ポート、MACアドレス又はユーザ名以外の他の基準によって決定される。従って、幾つかの実施例においては、VLANのメンバーシップは、例えば第2層パケットにおける所定のビットの値のようなパケットの内容に基づき決定される。スイッチ128が、1以上の値の予め決定されたセットの中にそのようなビットの値が存在するパケットを受取るとき、そのスイッチは、パケットの発信元MACアドレス、又はパケットが到達するポート160を対応するVLANに配置する。スイッチ128がルータに接続されたトランクポートにおけるパケットを送信する場合、スイッチはパケットにパケットのVLAN番号を付加する。ルータ130において、各VLAN番号はインタフェースに関連するものである。(この関係は、インタフェースが規定されたときに確立される。) 従って、図2に示すように、各ルータ130は、そのルータが直接接続される各IPサブネットに対する個別のインタフェース210を有する。付録B～Cの実施例と同様に接続グループが生成される。特にステップM 30に

において、管理者は、各接続グループに対して、どのようなパケットがその接続グループに属するかを決定するルールを指定する。例えば、所定のルールによって所定のビットの値を有するパケットが所定の接続グループに属することが決定され得る。

【0085】

幾つかの実施例においては、ルータ130におけるアクセス制御リストによって、IPアドレスとは別の基準に基づきトラフィックを許可するか或いは拒否する。例えば、或る基準にはポート番号が関係する（例えば、W. Cheswick及びFS、Bellovinの“Firewalls and Internet Security”（1994）、94-109頁を参照；ここで言及することにより本明細書の一部とする）。更に、所定の基準によって、インタフェースへのトラフィックよりも寧ろインタフェースからのトラフィックを指定する。管理者は、ステップM50の前に端末124Mに対して十分な情報を与え、そのような基準に従ってアクセス制御リストを作成する。

【0086】

幾つかの実施例においては、冗長(redundancy)を目的として、VLAN140が同一のルータの異なるインタフェース210に接続され得る。2つのインタフェースは、同一のサブネットか或いは2つの異なるサブネットに割当てられる。各ACLは、両方のインタフェースに対して同様の制限を与える。

【0087】

VLANが種々のルータのインタフェースに接続されるとき、場合によっては別のルータからアクセス可能な別の端末への情報の経路を指定するために、ルータの1つがVLANを経由して別のルータへデータを送信することを試みることができる。その場合、VLANに接続されたインタフェースに対するACLが、ルータ間のトラフィックを過度に制限しないように構築される。

幾つかの実施例においては、VLANサブネットは共用されるか或いは非管理であり、任意の接続グループのメンバではない。

【0088】

付録Gは、ネットワーク110において接続性を変更するためのメンテナンスプロセスを示す。付録Bのプロセスの再実行によって、任意の変更を行うことが

可能である。しかしながら、幾つかの実施例において付録G プロセスがメンテナンスを容易にする。

【0089】

幾つかの実施例において、ステップM50は省略される（ACLは生じない）。

【0090】

前述の実施例は本発明を限定するものではない。本発明は、特定のネットワーク、層、スイッチ、ルータ、オペレーティングシステム、或いは他のハードウェア若しくはソフトウェアに限定されるものではない。また本発明は企業ネットワークに限定されるものではない。幾つかの実施例においては、MACアドレスはNICに書込まれるものではなく、ソフトウェアによって生じる。幾つかの実施例において、付録B-Gの管理ソフトウェアの全て或いはその一部は端末124より寧ろスイッチ128又はルータ130で実行される。ソフトウェアは幾つかの実施例に適用される。

【0091】

幾つかの実施例においては、ドメイン116は第2層プロトコルとは別のプロトコルを使用し、ルータ130は、第3層プロトコルとは別のプロトコルに基づきトラフィックの経路指定を行う。各ドメインにおける接続性は、MACアドレス又は第2層パケットの内容とは別の情報に基づき決定され、ルータ130は、IPアドレスとは別の情報に基づきトラフィックを許可又は拒否する。幾つかの実施例においては、ルータ130はIPXアドレスを使用する。幾つかの実施例においては、D. Biererらの“NetWare 4 for Professionals” (1993)（ここで言及することにより本明細書の一部とする）に記載のネットワークウェア若しくはアップルトークネットワークを使用する。他の実施例及び変更例は、添付した請求の範囲によって規定される本発明の範囲内である。

付録A

ユーザベースネットワークコントロール (UBNC)

幾つかの実施例において、VLANのメンバーシップは端末にロケオンしたユーザに基づき決定される。Windows NT[®]の幾つかの実施例においては、UBNCサーバが全てのVLANからアクセス可能なように設置される（例えば、サーバが共用サブネ

ット内にある)。ネットワーク端末が能力アップされた(powered up)とき、それは「デフォルト(default)」VLANに配置される(デフォルトVLANは各々の第2層ドメイン116に存在する)。端末は、デフォルトVLANを提供するDHCPサーバからIPアドレスを受取る。ユーザが端末にログオンした時、端末はUBNCサーバに対して、ログオン時に与えられたユーザ名に関連するVLANに端末を切替えるように要求を送る。その要求には、ユーザ名、端末のMACアドレス、及び端末の現在のIPアドレスが含まれる。UBNCサーバは、UBNCサーバデータベースから関連するVLANを決定する。或る実施例においては、各ユーザ名に対して、データベースには関連するVLANの識別子が含まれる。別の実施例においては、データベースには管理端末によって与えられる以下のような情報が含まれる。

【0092】

- (A) 各ユーザ名について、そのユーザ名が属する接続グループの識別子
- (B) 各接続グループに属するVLANの識別子
- (C) 各VLANについて、関連するサブネット

UBNCサーバが要求を受取ると、サーバは要求する端末に対して(1)端末が異なるVLANに切替えられるかどうかの指示(端末がデフォルトVLANにないときにユーザがログオンした場合、切替が要求されない可能性があり、またVLANが規定されていないレイヤ2 BDにユーザがログオンした場合、切替が行われない可能性がある。)、並びに(2)ユーザに割当てられたVLANのIPサブネット及びサブネットワークを送信する。次にUBNCサーバは、端末がそのDHCPリース(DHCP lease)を解放するのを待つ。ここでUBNCサーバは、端末を含む第2層ドメイン116における単一のスイッチ又は複数のスイッチ128に対して適切なコマンドを送信する。そのスイッチによって、ユーザに割当てられたVLANに端末が配置される。

【0093】

UBNCサーバからの応答を受取った後に、端末はそのDHCPリースを解放し、次にサーバが端末を割当てられたVLANに切替え可能なように所定の期間待つ。その期間の後に、端末は切替が完了したと想定し、新たなDHCPリースの要求を送出する。応答において、端末は新たなIPアドレスを受取る。端末は新たなIPをUBNCサーバから受取ったサブネットワーク及びIPサブネットと照合する。新たなIPがサブ

ネットに存在しない場合、端末は新たな要求をUBNCサーバに対して送出することによってその手続きを繰り返す。端末が新たなIPを要求したときに端末が割当てられたVLANに切替えられていない場合、新たなIPは間違ったサブネットに存在する可能性がある。

【0094】

幾つかの実施例においては、デフォルトVLANは省略される。別の実施例においては、全ての端末又は地理的にもっとも近い端末のグループが個別のデフォルトVLANに割当てられ、UBNCサーバによってユーザがそれらと関連するVLANに切替えられるまで通信を制限する。ユーザがログオフした時、ユーザ端末は適切なデフォルトVLANに戻される。

付録B

接続グループ(Connectivity Groups)の生成

M.5 管理端末124Mにネットワーク110のIPアドレスレンジ（例えば、10.0.0/8）を与える。

M.7 管理端末124Mに情報12（付録C）を与える。

M.10 VLANを定義する。

M.14 第2層 BDにIPサブネットを割当てる。

M.20 各接続グループに対して、管理端末にグループのIPサブネットメンバを与える。1つの接続グループを管理接続グループとして指定する。

M.30 接続グループに管理可能なエンティティ（ポート、MACアドレス及び／又はユーザ名）を割当てる。

M.40 管理端末に情報17及び18を与える

M.45 管理端末124Mが、エンティティを適切なVLANに配置する（付録D参照）。

M.50 管理端末124Mが、ルータのためのアクセス制御リストを作成する（付録E参照）。

付録C

管理端末データベース

I.1 ネットワーク110のIPアドレスレンジ

1.2. 各ドメイン116について

1.2-1. ドメイン116における全てのVLAN-capableスイッチ128のIPアドレス

1.2-2. 各スイッチの非トランクポート160の識別子

1.3. 各ドメイン116について、ドメインにおけるVLANの識別子

1.4. 各第2層 BDについて、BDがVLANであるか否か、またIPサブネットがBDに含まれているか否かの指示。BDがVLANである場合、VLANの識別子。

1.5. 各接続グループについて、その接続グループに属するIPサブネット

1.6. 各接続グループについて、その接続グループに属するエンティティ（ポート、MACアドレス、及び／又はユーザ名）

1.7. 各ルーティングフェースについて

1.7-1. 関連するサブネット（仮に存在すれば）

1.7-2. インタフェースがVLAN-capable第2層ドメインに接続されているか否かを指示するフラッグ

1.8. ネットワーク110における全ての共用サブネットのリスト

付録D.VLANの生成

各接続グループCGについて、また接続グループにおける各エンティティE（16）について、

V.1. エンティティEがVLAN-capableスイッチ128のポート160である場合、

V.1-1. ポートが属するドメイン116-E（116P、116Q、116Rの1つ）を検索する（12-2、12-1）

V.1-2. 接続グループCG及びドメイン116-Eの両方におけるVLANを検索する（13、14、15）

V.1-3. ドメイン116-Eのスイッチ128又はドメイン116-Eの制御スイッチ128に対してコマンドを送信することによってポートEをVLANに配置する

V.2. 或いはエンティティEがMACアドレスである場合、接続グループCGにおけ

る各VLANについて（14、15）、

V2-1 VLANを含むドメイン116-V（116T、116Q、116Rの1つ）を決定する（13）

V2-2 ドメイン116-Vの制御スイッチ128又は全てのスイッチ128に対して適切なコマンドを送信することによってMACアドレスE5VLANに配置する

V3 或いはエンティティEがユーザ名である場合、

実施例1：接続グループCGにおける各VLANについて（14、15）、

V3-1 VLAN（13）を含むドメイン116-Vを決定する

V3-2 VLAN識別子、ドメイン116-Vの識別子、及びユーザ名をUBNCサーバに対して送信する

実施例2：

V3-1 接続グループCGの識別子及びユーザ名をUBNCサーバに送信する

付録E

ステップM50：リクエストに対するアクセス制御リストの生成

ネットワーク110における各ルータについて（12-3）、またルータの各インタフェースについて（17）、インタフェースと接続されたサブネットワークが接続グループに属する場合、

A1 各共用サブネットワークからのトラフィックを許可する（18）

A2 同一の接続グループにおける全ての別のサブネットワークからのトラフィックを許可する（15、14）

A3 ネットワーク110における他の全ての別のサブネットワークからのトラフィックを拒否する（11）

A4 ネットワーク110の外部からのトラフィックを許可する

A5 ルータにおいてTelnetセッションを開放し、ルータに対して以下を送信する

（1）インタフェースから存在するACL（もし存在すれば）を取除くためのコマンド（例えば、非アクセスグループ1）

（2）アクセスリスト

(3) コマンド:

```
interface vlan_e
access-group 1 out
```

これらのコマンドにより、ACLが「vlan_e」と標識されたルーティンタプフェースに対して割当てられる

付録 E

VLAN 140 e に対するルーティンタプフェース 210 のためのアクセス制御リスト

ACL 1-1 アクセスリスト 1 許可 ip 10.3.4.0 0.0.0.255

! 共用サブネット

ACL 1-2 a アクセスリスト 1 許可 ip 10.1.2.0 0.0.0.255

! 同一のものにおけるサブネット

! 企業の接続グループ

ACL 1-2 b アクセスリスト 1 許可 ip 10.3.2.0 0.0.0.255

! 同一のものにおけるサブネット

! 企業接続グループ

ACL 1-3 アクセスリスト 1 拒否 ip 10.0.0.0 0.255.255.255

! ネットワーク 110 における全てのサブネット

! 同一の接続グループの外部

ACL 1-4 アクセスリスト 1 許可 ip 任意

! からのアクセスの許可

! ネットワーク 110 の外部

付録 Gメンテナンシアプローチズ非管理から接続グループのメンバへのサブネットの変更

サブネットが 1 以上のゲートウェイアドレスを有する場合、サブネットは接続グループのメンバに変更されない。さもなければ、サブネットを接続グループに付加し、付録 E に示すように、同一の接続グループにおけるサブネットが直接接続される各々のインタプフェースに対するアクセス制御リストを再生成する。

非管理から共用へのサブネットの変更

共用サブネットのリスト18（付録C）にサブネットを付加する。付録Eに示すように、任意の接続グループにおけるサブネットが接続される各ルーティングフェーズのアクセス制御リストを再生成する。（サブネットは各ACLに付加され得る。）

共用から非管理へのサブネットの変更

共用サブネットのリスト18（付録C）からサブネットを除去する。付録Eに示すように、任意の接続グループにおけるサブネットが接続される各ルーティングフェーズのアクセス制御リストを再生成する。（サブネットは各ACLから除去され得る。）

共用から接続グループのメンバへのサブネットの変更

サブネットが1を越えるゲートウェイアドレスを有する場合、サブネットは接続グループのメンバに変更されない。さもなければ、サブネットを共用サブネット（付録C）のリスト18から除去し、またサブネットを接続グループ（付録C）における14）に付加する。付録Eに示すように、任意の接続グループにおけるサブネットが接続される各ルーティングフェーズのアクセス制御リストを再生成する。

接続グループのメンバから非管理へのサブネットの変更

接続グループ（付録Cの15）からサブネットを除去する。付録Eに示すように、同一の接続グループにおけるサブネットが直接接続される各ルーティングフェーズのアクセス制御リストを再生成する。（サブネットは各ACLから除去され得る。）付録Eに示すように、サブネットは直接接続されたルーティングフェーズに対するACLを除去し、次に（必要ならば）再生成する。（インタフェースに直接接続された他のサブネットが存在しない場合は、ACLは生成されない。別の単一のサブネット又は複数のサブネットが存在する場合は、適切なACLが生成される。）

接続グループのメンバから共用へのサブネットの変更

接続グループ（付録Cにおける15）からサブネットを除去する。サブネットが直接接続されているルーティングフェースに対するACLを除去する。付録Eに示すように、任意の接続グループにおけるサブネットが直接接続されている各ル

インタフェースのアクセス制御リストを再生成する。(サブネットは、グループのメンバとして幾つかのACLから取除かれるが、共用サブネットとして各ACLに付加される。)

1つの接続グループ(「旧」グループ)から別のグループ(「新」グループ)へのサブネットの移行

サブネットを旧グループから取除き、新グループ(付録Cの1.5)に付加する。付録Eに示すように、古い又は新規の接続グループの何れかにおけるサブネットが直接接続された各ルータインタフェースのACLを再生成する。

接続グループへの通信エンティティ(ポート、MACアドレス、ユーザ等)の付加(ステップM3.0参照)

管理者は、新しいエンティティが属すべき接続グループを指示する。

【0095】

ポート1.6.0 ポートはスイッチ1.2.8に接続され、それはそれ自体が第2層ドメイン1.1.6の一部である。所定の第2層ドメインにおいて、選択された接続グループは特定のサブネットと接続され、それは、それ自体が特定のVLANと結ばれる。ポートが接続グループに割付けられる際に、ステップV1(付録D)が実行され、ポートが第2層ドメインにおける接続グループのメンバであるVLANに配置される。マルチポートモジュールがスイッチに付加される場合には、或いは全部のスイッチがネットワークに付加される場合には、通常はポートがグループに付加されることに注目されたい。これらの場合において、新しいポートの全てのセットが、管理者によって選択された接続グループに付加される。次に(もし必要ならば)管理者は1つずつポートの割当を変更することができる。

【0096】

MACアドレス ポートに関する場合には、特定の第2層ドメインにおいて、選択された接続グループがサブネット/VLANペアに接続される。各第2層ドメインに対して、ステップV2(付録D)によって、所定のMACアドレスが指定されたVLANに割当てられるように、全てのスイッチ(又はスイッチの能力次第で、単一の制御スイッチ)が形成される。

【0097】

ユーザ。付録DのステップV3を参照。

或る接続グループ（「旧」グループ）から別のグループ（「新」グループ）への通信エンティティ（ポート、MACアドレス、ユーザ）の移行（ステップM30参照）。

ポート160 ポートはVLAN-capableスイッチ128に接続され、それはそれ自体が第2層ドメインの一部である。第2層ドメインにおいて、新旧の接続グループは特定のサブネットに接続され、それは、それら自体が特定のVLANに結ばれる。（新しい接続グループに属する第2層ドメインにおいてサブネットが存在しない場合、変更は行われない。）管理端末124Mは、新しいVLANに対するポートのVLANの割当を変更する。

【0098】

MACアドレス ポートの場合のように、特定の第2層ドメインにおいて、新規の接続グループはサブネット/VLANペアに関連する。各第2層ドメインについて、所定のMACアドレスが指定されたVLANに割当てられるように、端末124Mが全てのスイッチ（又はスイッチの能力次第で、単一の制御スイッチ）を構成する。特定の第2層ドメインにおける要求された接続グループに対応するサブネットが存在しない場合、第2層ドメインにおけるMACアドレスに対するVLANの割当は行われない。移行の結果として、或いは第2層ドメインにプラグインされたラップトップ又は他のモバイルコンピュータにMACアドレスが割当てられるために、MACアドレスが第2層ドメインに生じた場合、そこでスイッチは未知のMACアドレスが発生したときに、それらが通常とり得る全ての動作をとり得る。

【0099】

ユーザ 付録DのステップV3を参照。

新規のルーティングフェース/VLAN/サブネットの付加

新規のルーティングフェース210が、直接接続されたサブネットを含まない場合（ゲートウェイアドレスがない場合）、動作は要求されない。さもなければ、インタフェースは1以上のゲートウェイアドレス及び対応する直接接続されたサブネットを有する。直接接続された各サブネットについて、

1. サブネットが既に接続グループのメンバである（従って、別のルーティング

インタフェースに直接接続されている) 場合、サブネットは共用サブネットに変更される。前述の接続グループのメンバーから共用サブネットへサブネットを変更するためのプロセスを参照されたい。

【0100】

2、或いはサブネットが共用又は非管理として既に指定されている場合、動作は要求されない。

【0101】

3、或いはサブネットは新規のサブネットである。サブネットを共用サブネットのリスト18 (付録C) に付加する。付録Eに示すように、任意の接続グループにおけるサブネットが直接接続された各ルータインタフェースのアクセス制御リストを再生成する。(サブネットは共用サブネットとして各ACLに付加され得る。) サブネットがVLAN-capableスイッチ128を含む第2層ドメインに存在する場合、新規のVLANがドメインの中に生成され、新規のサブネットと接続される。

新規のルータの付加

新規のルータ130は幾つかのインタフェースを有し得る。各ルータインタフェースに対して、新規のルータインタフェースのためにリストされた動作が実行される。

新規のVLAN-capableスイッチの付加

新規のVLAN-capableスイッチ128が第2層ドメインに付加され、ここでは管理接続グループに割当てられたサブネットが存在し、またこのグループに対応するVLANが存在する。

【0102】

スイッチが、ポートベースVLAN(port-based VLANs)を具現する場合、スイッチの管理スタック及びスイッチにおける全てのポートは、管理接続グループにおけるサブネットに対応するVLANに割当てられる。更に、スイッチはこのサブネットからのIPアドレスに割当てられる。例えば、サブネット10.50.3.0/24が、管理グループに割当てられた第2層ドメインにおけるサブネットである場合、またVLAN3が、サブネット10.50.3.0/24に関連するVLANである場合、管理接続グループに

おけるアドレスに割当てするために、Cisco Catalyst 5000シリーズスイッチのコンソールにおいて次のようにコマンドを発行する。

【0103】

```
set interface sc0 3 10.50.3.200 255.255.255.0 10.50.3.255
```

ここでsc0は、スイッチの管理スタックに対する指名字であり、3は、サブネット10.50.3.0/24に対応するVLANであり、10.50.3.200は、スイッチの管理スタックに割当てられたサブネット10.50.3.200/24におけるIPアドレスであり、255.255.255.0は、サブネット10.50.3.0/24に対するサブネットマスクであり、更に10.50.3.255は同報通信アドレスである。

【0104】

スイッチがMACアドレスベースVLANを具現する場合、管理スタックのMACアドレスは、管理接続グループにおけるサブネットに対応するVLANに割当てられる。ポートベースVLANの場合のように、スイッチはこのサブネットからのIPアドレスに割当てられる。

新規の接続グループの付加

新規の（空の）接続グループは常に付加され得る。サブネットを接続グループにどのようにに付加するかについては前述の通りである。

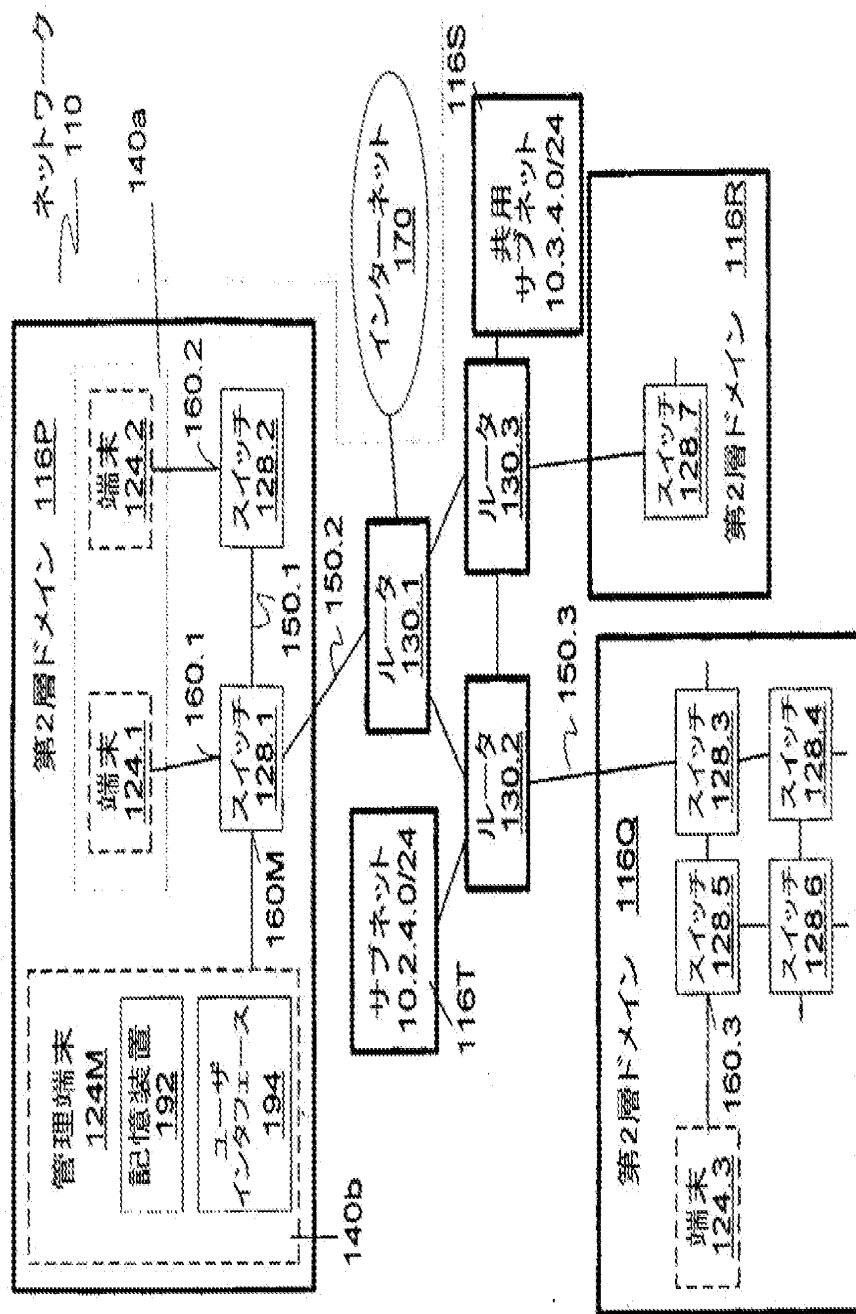
【図面の簡単な説明】

【図1】

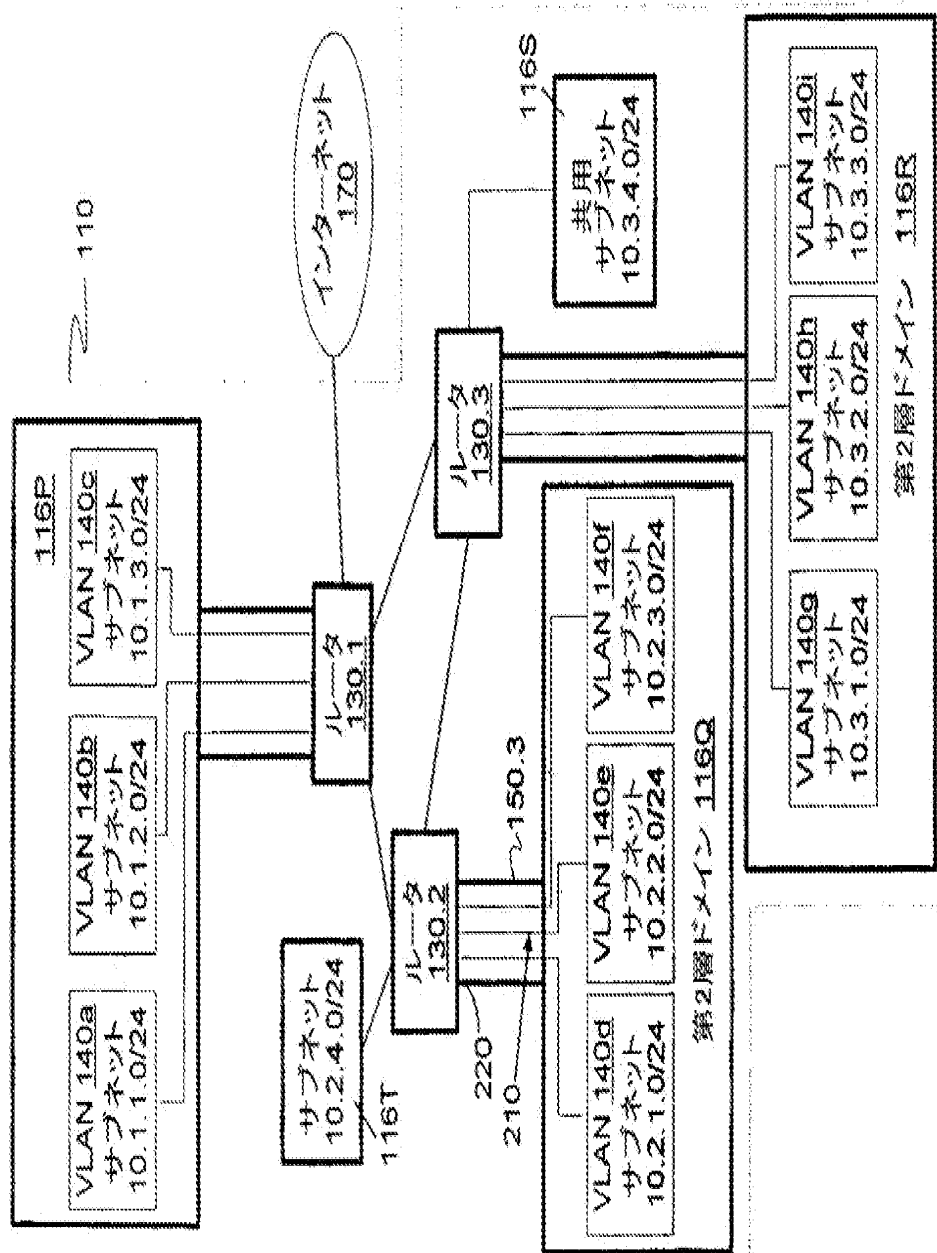
本発明により接続を確立したネットワークのブロック線図である。

【図2】

図1のネットワークにおけるVLAN及びルーティンタフェースを示すブロック線図である。



【図2】



【手続補正書】 特許協力条約第34条補正の翻訳文提出書

【提出日】 平成12年4月12日（2000、4、12）

【手続補正1】

【補正対象書類名】 明細書

【補正対象項目名】 特許請求の範囲

【補正方法】 変更

【補正内容】

【特許請求の範囲】

【請求項1】 ネットワーク端末をバーチャル同報通信ドメイン（VBDs；

140a乃至140i）に接続するための方法であって、

ネットワーク上においてネットワーク端末のユーザを識別する情報を前記ネットワーク端末から受信する過程と、

ユーザを識別する情報から1以上のVBDを含むユーザの属する接続グループを決定する過程と、

前記ネットワーク端末が接続される1以上のVBDを決定する過程であって、前記1以上のVBDが前記接続グループのメンバーであるような前記決定過程と、

前記ネットワーク端末を前記1以上のVBDに接続するためのコマンドを発行する過程とを含むことを特徴とする方法。

【請求項2】 各VBDが、前記トラフィックが生じる前記VBDへの同報通信トラフィックを制限可能なドメイン（116P）のサブドメインであり、

前記接続グループが、少なくとも2つのドメインからのVBDを含み、

前記ネットワーク端末が接続された1以上のVBDが、前記ネットワーク端末を含む前記ドメインに基づき決定されることを特徴とする請求項1に記載の方法。

【請求項3】 各VBDがVLANであり、また前記ネットワーク端末が、前記接続グループに属するVLAN並びに前記ネットワーク端末を含む前記ドメインに接続されることを特徴とする請求項2に記載の方法。

【請求項4】 ネットワーク端末をバーチャル同報通信ドメイン（VBDs；

140）に接続するための構造体であって、

ネットワーク上においてネットワーク端末のユーザを識別する情報を前記ネッ

トワーク端末から受信する手段と、

ユーザを識別する情報から1以上のVBDを含むユーザの属する接続グループを決定する手段と、

前記ネットワーク端末が接続される1以上のVBDを決定する手段であって、前記1以上のVBDが前記接続グループのメンバーであるような前記決定手段と、

前記ネットワーク端末を前記1以上のVBDに接続するためのコマンドを発行する手段とを含むことを特徴とする構造体。

【請求項5】 各VBDが、前記トラフィックが生じる前記VBDへの同報通信トラフィックを制限可能なドメイン（116P）のサブドメインであり、

前記接続グループが、少なくとも2つのドメインからのVBDを含み、

前記ネットワーク端末が接続された1以上のVBDが、前記ネットワーク端末を含む前記ドメインに基づき決定されることを特徴とする請求項4に記載の構造体。

【請求項6】 各VBDがVLANであり、また前記ネットワーク端末が、前記接続グループに属するVLAN並びに前記ネットワーク端末を含む前記ドメインに接続されることを特徴とする請求項5に記載の構造体。

【請求項7】 前記構造体が、（1）所定のコンピュータシステム（124M）、及び（2）前記コンピュータシステムにロードされた所定のプログラムを含み、前記コンピュータシステム及び前記プログラムが、前記決定手段の各々を含むことを特徴とする請求項4に記載の構造体。

【請求項8】 前記構造体が、所定のコンピュータの読取り可能な媒体であり、そこで各手段が、1以上のコンピュータの命令、コンピュータの読取り可能なデータ、又は1以上の命令及びデータの組合せを含むことを特徴とする請求項4に記載の構造体。

【請求項9】 ネットワークドメイン（116P、116Q、116R、116S、116T）間のトラフィックの経路を指定する1以上の装置（130）に対して1以上のアクセス制御リスト（ACLs）を生成するための方法において、そのような装置にACLが与えられた場合に、前記装置が、前記ACLを用いて前記ドメイン間においてどのようなトラフィックが許可及び／又は拒否されるかを決定し、更に、

サブネットワークの各グループ内においてトラフィックが許可されるように、サブネットワーク（140a、116T）の1以上のグループを規定する過程であって、各サブネットワークがネットワークドメインの一部であるか、或いはネットワークドメインの全でであり、また各グループに対して、所定のコンピュタシステムに前記グループに属するサブネットワークの識別子を与えるような前記過程と、

前記コンピュタシステムが、各グループ内のトラフィックを許可するため1以上のACLを生成する過程とを含むことを特徴とする方法。

【請求項10】 前記1以上のACLが異なるグループにおけるサブネットワーク間のトラフィックを拒否する前記複数のグループを規定する過程を含むことを特徴とする請求項9に記載の方法。

【請求項11】 1以上の共用サブネットワークの識別子を受信する前記コンピュタシステムを更に含む前記方法において、トラフィックが、前記グループの何れか1つにおける各共用ネットワークと任意の別のサブネットワークの間において許可され、

1以上のACLによって、トラフィックが、前記グループの何れか1つにおける前記共用サブネットワークの何れか1つと任意のサブネットワークとの間において許可されることを特徴とする請求項9に記載の方法。

【請求項12】 少なくとも1つの前記ドメインが、前記ドメインにおけるトラフィックを制限することが可能であるような前記方法であって、

1以上のグループの各々に対して、前記コンピュタシステムが、前記グループ内において許可及び／又は拒否されたトラフィックを識別するための情報を受信する過程であって、前記情報が、制限するトラフィックにおける1以上のドメインによって使用されるような前記受信過程と、

前記情報による指定に従ってトラフィックを許可及び／又は拒否するように、前記コンピュタシステムがトラフィックを制限可能な各ドメインを構成する過程とを更に含むことを特徴とする請求項9に記載の方法。

【請求項13】 所定のグループ内において許可及び／又は拒否されたトラフィックを識別するための情報が、1以上の（1）トラフィックを制限可能な

ドメイン内のトラフィックを各々送信する1以上のスイッチ（128）のポート（160）であって、前記グループ内のトラフィックを運ぶための前記ポート（160）と、（2）前記グループに属するエンティティ（124）の物理的アドレスと、更に（3）前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項12に記載の方法。

【請求項14】 各サブネットワークの識別子が、アドレス又はアドレスレンジであることを特徴とする請求項9に記載の方法。

【請求項15】 前記1以上の装置が、IPアドレスに基づきトラフィックの経路を指定し、また各ドメイン内において、トラフィックが物理的アドレスに基づき端末間で送信されることを特徴とする請求項9に記載の方法。

【請求項16】 ネットワークドメイン（116P、116Q、116R、116S、116T）間のトラフィックの経路を指定する1以上の装置（130）に対して1以上のアクセス制御リスト（ACLs）を生成するための所定の構造体において、そのような装置にACLが与えられた場合に、前記装置が、前記ACLを用いて前記ドメイン間においてどのようなトラフィックが許可及び／又は拒否されるかを決定し、更に、

各グループ内においてトラフィックが許可されるように、サブネットワーク（140、116）の1以上のグループをコンピュータシステムに対して規定する手段であって、各サブネットワークがネットワークドメインの一部であるか、或いはネットワークドメインの全てであり、また各グループに対して、前記グループに属するサブネットワークの識別子をコンピュータシステムによって読取るための前記規定手段と、

前記コンピュータシステムによって、各グループ内のトラフィックを許可するために1以上のACLを生成するための手段とを含むことを特徴とする構造体。

【請求項17】 前記構造体が、前記コンピュータシステム（124M）及び該コンピュータシステムにロードされた所定のプログラムの含み、前記コンピュータシステムと前記プログラムの組合せが、前記規定手段及び生成手段を含むことを特徴とする請求項16に記載の構造体。

【請求項18】 前記構造体が、前記規定手段及び前記生成手段を実施す

るための命令を含むコンピュータの読取り可能媒体であることを特徴とする請求項16に記載の構造体。

【請求項19】 前記規定手段が複数のグループを規定するときに、前記1以上のACLが異なるグループにおけるサブネットワーク間のトラフィックを拒否することを特徴とする請求項16に記載の構造体。

【請求項20】 1以上の共用サブネットワーク（116S）の識別子を前記コンピュータシステムによって読取るための手段を更に含む前記構造体において、前記グループの何れか1つにおける各共用サブネットワークと他の任意のサブネットワークとの間でトラフィックが許可され、

1以上の前記ACLによって、前記グループの何れか1つにおける前記共用サブネットワークの何れか1つと任意のサブネットワークとの間でトラフィックが許可されることを特徴とする請求項16に記載の構造体。

【請求項21】 少なくとも1つの前記ドメインが、前記ドメインにおけるトラフィックを制限可能であるような前記構造体であって、

1以上のグループの各々に対して、前記グループ内における許可及び／又は拒否されたトラフィックを識別するための情報を前記コンピュータシステムによって読取るための手段であって、前記情報が、トラフィックの制限において1以上のドメインによって使用されるような読取り手段と、

前記情報による指定に従ってトラフィックを許可及び／又は拒否するように、トラフィックを制限可能な各ドメインを前記コンピュータシステムによって構成するための手段とを更に含むことを特徴とする請求項16に記載の構造体。

【請求項22】 所定のグループ内において許可及び／又は拒否されたトラフィックを識別するための情報が、1以上の（1）トラフィックを制限可能なドメイン内のトラフィックを各々送信する1以上のスイッチ（128）のポート（160）であって、前記グループ内のトラフィックを運ぶための前記1以上のポート（160）と、（2）前記グループに属するエンティティの物理的アドレスと、更に（3）前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項21に記載の構造体。

【請求項23】 各サブネットワークの識別子が、アドレス又はアドレス

レンジであることを特徴とする請求項16に記載の構造体。

【請求項24】 前記1以上の装置が、IPアドレスに基づきトラフィックの経路を指定し、また各ドメイン内において、トラフィックが物理的アドレスに基づき端末間で送信されることを特徴とする請求項16に記載の構造体。

【請求項25】 複数のドメイン(116)を含む所定のネットワークにおける接続を確立するための方法において、

各ネットワーク端末が、第1の型のアドレス及び第2の型のアドレスを有することが可能であり、

各ドメインにおけるネットワーク端末間のトラフィックが、宛先ネットワーク端末の第2の型のアドレスを用いることなしに、前記宛先ネットワーク端末の第1の型のアドレスを使用して前記宛先ネットワーク端末に送信され、一方でドメイン間においては、前記宛先ネットワーク端末の第2の型のアドレスを使用してトラフィックが送信され、また制限され、

ドメインが単一のサブドメイン内のトラフィックを許可し、一方でサブドメイン間のトラフィックを拒否するように、少なくとも1つのドメインが、前記ドメインにおいて規定されたサブドメイン(140)を有することが可能であり、更に、

接続グループCG1に属するトラフィックを規定する情報INF1をコンピュータシステム(124M)に与える過程であって、前記接続グループCG1が、種々のドメインにおいてサブドメインを有するためのものであり、それらの少なくとも2つがサブドメインへのトラフィックをそれぞれ制限可能であるような前記過程と、

少なくとも前記接続グループCG1について、ドメインが、前記第2の型のアドレスを用いることなしに前記第1の型のアドレスを使用してトラフィックを送信するときに、前記ドメインD1が前記情報INF1によって規定されたトラフィックを許可し、一方でサブドメインSD1へのそのようなトラフィックを制限するように、前記コンピュータシステムが、前記接続グループCG1におけるサブドメインSD1を有する各ドメインD1を生成する過程とを含むことを特徴とする方法。

【請求項26】 トラフィックを規定する前記情報が、少なくとも1つのグループに対して、1以上の(1) 単一のドメイン内のトラフィックを各々送信する1以上のスイッチ(128)のポート(160)であって、前記グループ内のトラフィックを運ぶための1以上の前記ポート(160)と、(2) 前記グループのメンバである端末(124)の物理的アドレスと、更に(3) 前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項25に記載の方法。

【請求項27】 各々のドメインを構成する過程が、前記グループにおけるサブドメインを有する単一のドメイン内のトラフィックを送信するスイッチについて、(a) 前記グループのメンバである端末の物理的アドレス間のトラフィックを許可するための、また(b) 異なるグループのメンバである端末の物理的アドレス間のトラフィックを拒否するための前記スイッチを構成する過程を含むことを特徴とする請求項26に記載の方法。

【請求項28】 複数のドメイン(116)を含む所定のネットワークにおける接続を確立するための構造物において、

各ネットワーク端末が、第1の型のアドレス及び第2の型のアドレスを有することが可能であり、

各ドメインにおけるネットワーク端末間のトラフィックが、宛先ネットワーク端末の第2の型のアドレスを用いることなしに、前記宛先ネットワーク端末の第1の型のアドレスを使用して前記宛先ネットワーク端末に送信され、一方でドメイン間においては、前記宛先ネットワーク端末の第2の型のアドレスを使用してトラフィックが送信され、また制限され、

ドメインが単一のサブドメイン内のトラフィックを許可し、一方でサブドメイン間のトラフィックを拒否するように、少なくとも1つのドメインが、前記ドメインにおいて規定されたサブドメイン(140)を有することが可能であり、更に、

接続グループCC1に属するトラフィックを規定する情報INF1をコンピュータシステム(124M)によって受信するための手段であって、前記接続グループCC1が、種々のドメインにおいてサブドメインを有するためのものであり

、それらの少なくとも2つがサブドメインへのトラフィックをそれぞれ制御可能であるような前記受信手段と、

少なくとも1つの接続グループについて、前記接続グループのメンバであるサブドメインの識別子を前記コンピュータシステムによって受信する手段と、
 少なくとも前記接続グループCG1について、ドメインが、前記第2の型のアドレスを用いることなしに前記第1の型のアドレスを使用してトラフィックを送信するときに、前記ドメインD1が前記情報INF1によって規定されたトラフィックを許可し、一方でサブドメインSD1へのそのようなトラフィックを制限するように、前記接続グループCG1におけるサブドメインSD1を有する各ドメインD1を前記コンピュータシステムによって構成するための手段とを有することを特徴とする構造体。

【請求項29】 トラフィックを規定する前記情報が、少なくとも1つのグループに対して、1以上の(1)単一のドメイン内のトラフィックを各々送信する1以上のスイッチ(128)のポート(160)であって、前記グループ内のトラフィックを運ぶための1以上の前記ポート(160)と、(2)前記グループのメンバである端末(124)の物理的地址と、更に(3)前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項28に記載の構造体。

【請求項30】 前記構造体が、前記コンピュータシステム及び該コンピュータシステムにロードされた所定のプログラムを含み、前記コンピュータシステムと前記プログラムとの組合せが、前記全ての手段を含むことを特徴とする請求項28に記載の構造体。

【請求項31】 前記全ての手段を実施するための命令を含むコンピュータの読取り可能媒体であることを特徴とする請求項28に記載の構造体。

【請求項32】 各ドメイン内のトラフィックが、端末の物理的地址に基づき端末間で送信され、またドメイン間のトラフィックが、端末の論理的地址に基づき経路指定されることを特徴とする請求項28に記載の構造体。

【手続補正2】

【補正対象書類名】 明細書

【補正対象項目名】 0003**【補正方法】 変更****【補正内容】****【0003】**

これについて図1及び図2に示す（これらの図には先行技術にはない本発明の幾つかの態様が示してある）。ネットワーク110は、大規模な組織の相互接続に適する企業ネットワークである。ネットワーク110には、「第2層ドメイン（layer 2 domains）」116P、116Q、116R、116S、116Tが含まれる（用語「第2層」は、D. Biererらの“NetWare4 for Professionals”（1993）、19頁に記載のOSI参照モデルのを指す）。同一の第2層ドメイン116に属する端末124（例えば、ドメイン116Pにおける端末124.1、124.2）は、それらのMACアドレス（「第2層」アドレス）を用いて互いに通信可能である。MAC（媒体アクセス制御）アドレスは、端末のネットワークインターフェースカード（NIC）に書込まれた物理的アドレスであるか、又はNICスイッチの設定によって確立された物理的アドレスである。全てのドメイン116又はその幾つかには、1以上のネットワークスイッチ（NICスイッチと混同しない）が含まれ得る。各ドメイン116のスイッチ128は、端末のMACアドレスを用いて端末124間でトラフィックを送信する。

【手続補正3】**【補正対象書類名】 明細書****【補正対象項目名】 0023****【補正方法】 変更****【補正内容】****【0023】**

ユーザ名によるVLANのメンバーシップの確定については、付録Aに記載されている。（“User-Based Binding of Network Stations to Broadcast Domains”と題するJ. Ekstromらの米国特許第5,968,126号（1999年10月19日発行）を参照。これについては、ここで言及することにより本明細書の一部とする。）或る実施例においては、VLAN140が、ポートによって識別される端末、MACアドレスに

よって識別される端末、及び／又はユーザ名によって識別される端末を結び付ける。

INTERNATIONAL SEARCH REPORT

International Application No. PCT/JP 99/08666	
Classifications of documents considered to be relevant Classifications of documents, with indication of the relevant passages	
A	SAUNDERS S: "SWITCH PUTS VIRTUAL LANS ON AUTOMATIC PILOT. AGILE'S AMPLIFIER SWITCH IS THE FIRST TO AUTOMATE SETUP OF VIRTUAL WORKGROUPS" DATA COMMUNICATIONS Vol. 23, no. 12 1 September 1994 (1994-09-01), pages 45/46 XP000462380 ISSN: 0363-8399 the whole document
A	AXNER D H: "DIFFERING APPROACHES TO VIRTUAL LANS" BUSINESS COMMUNICATIONS REVIEW, 42-45, December 1993 (1993-12), pages 42-45. XP000669940 abstract
Referred to claims by: 7, 8, 13, 15, 17, 19, 22-24, 26, 27, 29-32 1, 4, 9, 16, 25, 28	

INTERNATIONAL SEARCH REPORT

Indicates an patent family members

Patent document cited in search report		Publication date	Patent family member(s)	Publication date	Publication date
WO 9802821	A	22-01-1998	AU GB	3728497 A 2330285 A	09-02-1998 14-04-1999
EP 0812086	A	10-12-1997	JP	10056473 A	24-02-1998

International Application No.
PCT/JP 99/08856

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(CH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW

(72)発明者 エクストロム、ジョセフ・ジェイ
 アメリカ合衆国ユタ州84042・リンドン、
 イースト 300サウス 131
 (72)発明者 モス、ステイブン・エス
 アメリカ合衆国ユタ州84042・リンドン、
 ノース 450-イースト 298

【要約の続き】
 によって制限される。